JOURNAL OF ALGEBRA 174, 523–530 (1995)

The Exact Lower Bound for the Degree of Commutativity of a p-Group of Maximal Class

GUSTAVO A. FERNÁNDEZ-ALCOBER*

Matematika Saila, Zientzi Fakultatea, Euskal Herriko Unibertsitatea, 644 Posta-kutxatila, Bilbo, Spain

Communicated by Peter M. Neumann

Received September 29, 1993

The most important invariant related to a p-group of maximal class G is its degree of commutativity $c(G)$, introduced by Blackburn in [1], which is a measure of the commutativity among the members of the lower central series of G. Suppose $|G| = p^m$ with p a prime and $m \geq 4$, and denote $G_i = \gamma_i(G)$ for $i \geq 2$ and $G_1 = C_G(G_2/G_4)$. Then, $c(G)$ can be defined as

$$c(G) = \max\{k \leq m - 2 | [G_i, G_j] \leq G_{i+j+k}\}.$$

So G_1 is abelian if and only if $c(G) = m - 2$.

In his above-mentioned pioneer paper, Blackburn showed that all 2-groups of maximal class satisfy $c(G) = m - 2$, whereas $c(G) \geq m - 4$ holds for $p = 3$ and $2c(G) \geq m - 6$ for $p = 5$. The importance of these lower bounds lies in the fact that they can be translated into structural properties of the group G. For example, if $\lambda \in \mathbb{N}$, $\mu \in \mathbb{Z}$, and $\lambda c(G) \geq m - \mu$, then the subgroup G_i has nilpotency class at most λ, where i is the smallest positive integer greater than or equal to $(\mu - 1)/(\lambda + 1)$. In particular, Blackburn's bounds yield that G_2 is abelian when $p = 3$ and has class at most 2 for $p = 5$.

These results were independently generalized to arbitrary primes by Shepherd [6] and Leedham-Green and McKay [3], who proved that $2c(G) \geq m - 3p + 6$ holds in any p-group of maximal class. It turns out that, for a fixed odd prime, G_{p-2} remains of class ≤ 2, however large the order of the group may become.

Blackburn's bound for 5-groups of maximal class is known to be best possible. This is not the case for the general lower bound $2c(G) \geq m - 3p + 6$, since Shepherd has proved that $2c(G) \geq m - 9$ holds for $p = 7$.

* This work has been supported by DGICYT Grant PB91-0446 and by the University of the Basque Country. E-mail: mtpfealg@lg.ehu.es.

0021-8693/95/ $6.00

Thus, the following problem arises: find the best bound of the type $2c(G) \geq m - g(p)$, in the sense that for every $p \geq 7$ there exists at least a p-group of maximal class whose degree of commutativity matches the bound. Examples constructed by Leedham-Green and McKay in [4] show that $g(p) \geq 2p - 5$. On the other hand, as the same authors prove (cf. [5]), if $p \geq 7$ and G_1 has class ≤ 2 then $2c(G) \geq m - 2p + 5$. Hence, $g(p) > 2p - 5$ if and only if there exist p-groups of maximal class in which G_1 has class at least 3 and $2c(G) < m - 2p + 5$.

The goal of this paper is to settle the question stated above by proving the following theorem.

THEOREM. *Let $p \geq 7$ be a prime number. If G is a p-group of maximal class of order p^m then $2c(G) \geq m - 2p + 5$.*

In order to prove the theorem, we need a definition and some lemmas. We note that, in the following, we will sometimes write just c instead of $c(G)$.

DEFINITION. Let p be a prime number and $f\colon S \to \mathbb{F}_p$ a function, where $S \subseteq \mathbb{Z}^2$. We call f a *p-maximal function* if the following properties hold whenever the values of f involved are defined:

P1. $f(i,j) = f(i,j+1) + f(i+1,j)$.

P2. $f(i,j) = -f(j,i)$.

P3. $f(i,j) = f(i+p-1,j) = f(i,j+p-1)$.

If G is a p-group of maximal class, we can take a couple of elements $s \in G - (G_1 \cup C_G(G_{m-2}))$ and $s_1 \in G_1 - G_2$, and define recursively $s_i = [s_{i-1}, s]$. We have $s_i \in G_i - G_{i+1}$ for $1 \leq i \leq m-1$ and $s_i = 1$ for $i \geq m$. If $c(G) < m - 2$ then we can define a function α over the set $\{(i,j) \in \mathbb{N}^2 | i + j \leq m - c - 1\}$ by means of the congruence

$$[s_i, s_j] \equiv s_{i+j+c}^{\alpha(i,j)} \pmod{G_{i+j+c+1}},$$

where we consider $\alpha(i,j)$ as an element of the field $\mathbb{F}_p$. Note also that, from the definition itself of the degree of commutativity, α cannot be the zero function. It is well known that α is a p-maximal function and that

$$\begin{aligned}\alpha(i,j)\alpha(i+j+c,k) + \alpha(j,k)\alpha(j+k+c,i) \\ + \alpha(k,i)\alpha(k+i+c,j) = 0 \end{aligned} \tag{1}$$

for $i + j + k \leq m - 2c - 1$ (see [3]).

LEMMA 1. *If $c(G) \leq m - p - 2$ then α can be extended to a p-maximal function with domain $\mathbb{N}^2$.*

It must be noted that, in Chapter 2 of R. Shepherd's thesis, where he develops some preliminary results in order to prove that the nilpotency class of G_1 is always less than or equal to $(p + 1)/2$, he defines the concept of a *table*, which differs only in one condition from the definition we have given for a p-maximal function and, in the end, is equivalent to it. Also, an alternative proof of Lemma 1 could be given from Proposition 2.4 in Shepherd's thesis.

Proof. For any $j \geq 1$, define $\beta(1, j) = \alpha(1, j_0)$, where $j_0 \in [1, p - 1]$ and $j \equiv j_0 \pmod{p - 1}$. Since P3 holds for α, it follows that $\beta(1, j) = \alpha(1, j)$ for $1 \leq j \leq m - c - 2$. Next, define $\beta(i, j)$ for all $i, j \geq 1$ inductively on i by means of $\beta(i, j) = \beta(i - 1, j) - \beta(i - 1, j + 1)$. Based on this relation, an easy induction on $r \geq 0$ shows that

$$\beta(i, j) = \sum_{k=0}^{r} (-1)^k \binom{r}{k} \beta(i - r, j + k), \qquad \text{for } i \geq r + 1, \tag{2}$$

and

$$\beta(i, j) = \sum_{k=0}^{r} (-1)^k \binom{r}{k} \beta(i + k, j - r), \qquad \text{for } j \geq r + 1. \tag{3}$$

From property P1, similar formulas can be derived for α, with the necessary restriction $i + j \leq m - c - 1$. In particular, setting $r = i - 1$ in (2) we get

$$\begin{aligned} \beta(i, j) &= \sum_{k=0}^{i-1} (-1)^k \binom{i - 1}{k} \beta(1, j + k) \\ &= \sum_{k=0}^{i-1} (-1)^k \binom{i - 1}{k} \alpha(1, j + k) = \alpha(i, j) \end{aligned}$$

for $i + j \leq m - c - 1$. Thus β is an extension of α.

Let us check that β is a p-maximal function. Property P1 is automatically satisfied from the definition of β. In order to prove that $\beta(i, j) = \beta(i, j + p - 1)$ we argue by induction on $i \geq 1$. This is true for $i = 1$ from the definition of the $\beta(1, j)$'s. If $i \geq 2$ then $\beta(i, j) = \beta(i - 1, j) - \beta(i - 1, j + 1) = \beta(i - 1, j + p - 1) - \beta(i - 1, j + p) = \beta(i, j + p - 1)$.

Now we see that $\beta(i,j) = \beta(i+p-1,j)$. If $i \geq 2$ then (2) with $r = p$ yields

$$\begin{aligned}\beta(i+p-1,j) &= \sum_{k=0}^{p} (-1)^k \binom{p}{k} \beta(i-1,j+k) \\ &= \beta(i-1,j) - \beta(i-1,j+p) \\ &= \beta(i-1,j) - \beta(i-1,j+1) = \beta(i,j).\end{aligned}$$

For $i = 1$ we use induction on j. If $j = 1$ then $\beta(1,1) = \alpha(1,1) = \alpha(p,1) = \beta(p,1)$, since P3 holds for α and $c \leq m - p - 2$ implies $p + 1 \leq m - c - 1$. On the other hand, for $j \geq 2$ we have $\beta(1,j) = \beta(1,j-1) - \beta(2,j-1) = \beta(p,j-1) - \beta(p+1,j-1) = \beta(p,j)$.

Finally, we prove that $\beta(i,j) = -\beta(j,i)$ for all $i,j \geq 1$. We proceed by induction on $i + j$. If $i + j \leq m - c - 1$ then β and α coincide and the result trivially holds. If, on the contrary, $i + j \geq m - c \geq p + 2$ then

$$\begin{aligned}\beta(i,j) &= \sum_{k=0}^{i-1} (-1)^k \binom{i-1}{k} \beta(1,j+k) \\ &= -\sum_{k=0}^{i-2} (-1)^k \binom{i-1}{k} \beta(j+k,1) + (-1)^{i-1} \beta(1,j+i-1) \\ &= -\sum_{k=0}^{i-2} (-1)^k \binom{i-1}{k} \beta(j+k,1) + (-1)^{i-1} \beta(1,j+i-p) \\ &= -\left\{ \sum_{k=0}^{i-2} (-1)^k \binom{i-1}{k} \beta(j+k,1) + (-1)^{i-1} \beta(j+i-p,1) \right\} \\ &= -\sum_{k=0}^{i-1} (-1)^k \binom{i-1}{k} \beta(j+k,1) = -\beta(j,i),\end{aligned}$$

where we have used (2) and (3) with $r = i - 1$, the induction hypothesis, and Property P3. ∎

LEMMA 2. *If $c(G) \leq m - p - 2$ then α can be extended to a p-maximal function with domain $\mathbb{Z}^2$.*

Proof. If $i,j \in \mathbb{Z}$, take $i_0, j_0 \in [1, p-1]$ such that $i \equiv i_0 \pmod{p-1}$ and $j \equiv j_0 \pmod{p-1}$. Then define $\gamma(i,j) = \beta(i_0,j_0)$, where $\beta\colon \mathbb{N}^2 \to \mathbb{F}_p$ is the p-maximal function obtained from α in Lemma 1. Clearly, γ is an extension of β and, hence, also of α. On the other hand, it is straightforward to check that γ is a p-maximal function. ∎

LEMMA 3. *Suppose that* $p \geq 7$. *If* $2c(G) \leq m - 2p + 4$ *and* $\gamma: \mathbb{Z}^2 \to \mathbb{F}_p$ *is the p-maximal function obtained from* α *in Lemma* 2, *then*

$$\Gamma(i,j,k) = \gamma(i,j)\gamma(i+j+c,k) + \gamma(j,k)\gamma(j+k+c,i) + \gamma(k,i)\gamma(k+i+c,j) = 0$$

for all $i, j, k \in \mathbb{Z}$.

Proof. First of all, note that $p \geq 7$ together with $2c(G) \leq m - 2p + 4$ implies $c(G) \leq m - p - 2$. Hence, it makes sense to speak of the function γ.

We observe that P2 implies $\gamma(i,i) = 0$ for any $i \in \mathbb{Z}$, since p is odd. Consequently, $\Gamma(i,j,k) = 0$ whenever any two of i, j, and k are equal. Moreover, if σ is any permutation of the set $\{i,j,k\}$ then $\Gamma(\sigma(i), \sigma(j), \sigma(k)) = \operatorname{sgn}(\sigma)\Gamma(i,j,k)$, where $\operatorname{sgn}(\sigma)$ denotes the signature of σ. Finally, it is clear that Γ is periodic in any of its three variables, with $p - 1$ as a period.

We prove that $\Gamma(i,j,k) = 0$ for all $i, j, k \in \mathbb{Z}$ in three steps.

First Step. $\Gamma(1,j,k) = 0$ for $j, k \geq 1$ and $j + k \leq 2p - 6$.

This case is immediate, since $1 + j + k \leq m - 2c - 1$ implies

$$\Gamma(1,j,k) = \alpha(1,j)\alpha(j+c+1,k) + \alpha(j,k)\alpha(j+k+c,1) + \alpha(k,1)\alpha(k+c+1,j) = 0,$$

according to (1).

Second Step. $\Gamma(1,j,k) = 0$ for $1 \leq j, k \leq p - 1$.

Since $\Gamma(1,j,j) = 0$ and $\Gamma(1,j,k) = -\Gamma(1,k,j)$, it suffices to consider $\Gamma(1, p-2, p-1)$, $\Gamma(1, p-3, p-1)$, $\Gamma(1, p-4, p-1)$, and $\Gamma(1, p-3, p-2)$.

From P1 for γ we easily derive that

$$\Gamma(r,j,k) = \Gamma(r+1,j,k) + \Gamma(r,j+1,k) + \Gamma(r,j,k+1).$$

Suppose that $i < j$. By letting r run from i to $j - 1$ in the previous equality and adding we get

$$\Gamma(i,j,k) = \sum_{r=i}^{j-1} \Gamma(r,j+1,k) + \sum_{r=i}^{j-1} \Gamma(r,j,k+1),$$

since $\Gamma(j, j, k) = 0$. By applying this last formula we obtain

$$\Gamma(i, p-2, p-1) = \sum_{r=i}^{p-3} \Gamma(r, p-1, p-1) + \sum_{r=i}^{p-3} \Gamma(r, p-2, p)$$
$$= \sum_{r=i}^{p-3} \Gamma(1, r, p-2) = \Gamma(1, p-3, p-2), \quad (4)$$

for $1 \le i \le p-3$. Also, if $1 \le i \le p-4$ then

$$\Gamma(i, p-3, p-1)$$
$$= \sum_{r=i}^{p-4} \Gamma(r, p-2, p-1) + \sum_{r=i}^{p-4} \Gamma(r, p-3, p)$$
$$= (p-3-i)\Gamma(1, p-3, p-2) + \sum_{r=i}^{p-4} \Gamma(1, r, p-3)$$
$$= (p-3-i)\Gamma(1, p-3, p-2). \quad (5)$$

On the other hand,

$$\Gamma(1, p-3, p-2)$$
$$= \sum_{r=1}^{p-4} \Gamma(r, p-2, p-2) + \sum_{r=1}^{p-4} \Gamma(r, p-3, p-1)$$
$$= \binom{p-3}{2} \Gamma(1, p-3, p-2) = 6\Gamma(1, p-3, p-2).$$

Since $p \ge 7$, it follows that $\Gamma(1, p-3, p-2) = 0$. Thus the expressions in (4) and (5) also equal zero. Hence it only remains to prove that $\Gamma(1, p-4, p-1) = 0$. This follows from

$$\Gamma(1, p-4, p-1) = \sum_{r=1}^{p-5} \Gamma(r, p-3, p-1) + \sum_{r=1}^{p-5} \Gamma(1, r, p-4).$$

Third Step. $\Gamma(i, j, k) = 0$ for all $i, j, k \in \mathbb{Z}$.

We first prove it for $i \ge 1$, by induction. Suppose $i = 1$. If $j \equiv j_0 \pmod{p-1}$ and $k \equiv k_0 \pmod{p-1}$ with $1 \le j_0, k_0 \le p-1$, then $\Gamma(1, j, k) = \Gamma(1, j_0, k_0) = 0$ follows from the previous step. If $i \ge 2$, the relation

$$\Gamma(i, j, k) = \Gamma(i-1, j, k) - \Gamma(i-1, j+1, k) - \Gamma(i-1, j, k+1)$$

completes the induction.

Now, if $i \leq 0$ it suffices to take $l \geq 1$ such that $l \equiv i \pmod{p-1}$ and note that $\Gamma(i,j,k) = \Gamma(l,j,k) = 0$. ∎

Proof of the Theorem. After these preliminary lemmas, the remainder of the proof of the theorem is the same as Leedham-Green and McKay's proof for the bound $2c(G) \geq m - 3p + 6$. We include it here for the sake of completeness.

Assume, by way of contradiction, that $2c(G) \leq m - 2p + 4$. Then Lemma 3 gives

$$\begin{aligned} 0 &= \Gamma(j+1, j, 1-c) \\ &= \gamma(j+1, j)\{\gamma(2j+c+1, 1-c) - \gamma(j+1, 1-c)\} \end{aligned} \tag{6}$$

for all $j \in \mathbb{Z}$, since $\gamma(j+1, j+1) = 0$ and $\gamma(j+2, j) = \gamma(j+1, j) - \gamma(j+1, j+1) = \gamma(j+1, j)$. On the other hand, if we write $x(i) = \gamma(i+1, i)$, induction on $k \geq 1$ yields

$$\gamma(i+k, i) = \sum_{r=0}^{[(k-1)/2]} (-1)^r \binom{k-r-1}{r} x(i+r). \tag{7}$$

By applying this formula to (6) for $j \geq 2 - c$, we get

$$x(j)\{(-1)^{j+c-1}(j+c)x(j) + \Sigma'\} = 0, \tag{8}$$

where Σ' denotes a linear combination of $x(j-1), \ldots, x(2-c)$. Since $j + c \not\equiv 0 \pmod{p}$ for $j = 2 - c, \ldots, p - 1 - c$, by substituting these values successively into (8) we obtain $x(2-c) = \cdots = x(p-1-c) = 0$. Furthermore, $x(1-c) = \gamma(2-c, 1-c) = -\gamma(p-c, 2-c) = 0$, since this last value is a linear combination of $x(2-c), \ldots, x(p-1-c)$, according to (7). It follows from P3 that $x(i) = 0$ for all $i \in \mathbb{Z}$. Now (7) implies $\gamma(i,j) = 0$ for any $i, j \in \mathbb{Z}$, which in turn yields $\alpha = 0$, a contradiction. ∎

This new bound for the degree of commutativity allows us to improve the corollaries deduced by Leedham-Green and McKay in [3] from the bound $2c(G) \geq m - 3p + 6$. We omit the proofs of the following results, since they are similar to those given in [3], once we have checked apart the primes 2, 3, and 5, which are not covered by the bound $2c(G) \geq m - 2p + 5$.

COROLLARY 1. *In any p-group of maximal class, G_i has nilpotency class ≤ 2, where i is the smallest positive integer greater than or equal to $(2p-6)/3$.*

For example, the subgroup of class ≤ 2 we get from the previous corollary for $p = 11$ is G_6, while the results up to now only yielded G_9.

COROLLARY 2. *If $m \geq 6p - 25$ then G_1 has nilpotency class at most* 3.

COROLLARY 3. *If $m \geq 6p - 37$ then the solubility length of G is at most* 3.

COROLLARY 4. *For $p \geq 3$, the solubility length of any p-group of maximal class is at most* $[\log_2(p-1)] + 1$.

In contrast with this last corollary, we note that, for p odd, Kovács and Leedham-Green have produced a family of p-groups of maximal class of order p^p and solubility length $[\log_2(p+1)]$ (cf. [2]).

REFERENCES

1. N. BLACKBURN, On a special class of p-groups, *Acta Math.* **100** (1958), 45–92.
2. L. G. KOVÁCS AND C. R. LEEDHAM-GREEN, Some normally monomial p-groups of maximal class and large derived length, *Quart. J. Math. Oxford Ser. (2)* **37** (1986), 49–54.
3. C. R. LEEDHAM-GREEN AND S. MCKAY, On p-groups of maximal class, I, *Quart. J. Math. Oxford Ser. (2)* **27** (1976), 297–311.
4. C. R. LEEDHAM-GREEN AND S. MCKAY, On p-groups of maximal class, II, *Quart. J. Math. Oxford Ser. (2)* **29** (1978), 175–186.
5. C. R. LEEDHAM-GREEN AND S. MCKAY, On p-groups of maximal class, III, *Quart. J. Math. Oxford Ser. (2)* **29** (1978), 281–299.
6. R. SHEPHERD, "p-Groups of Maximal Class," Ph.D. thesis, University of Chicago, 1970.